IN THE SPECIFICATION:

Please replace paragraph 6 at page 16, with the following rewritten paragraph:

an encrypted content encrypted on the basis of a second block key ~~Kb1~~ Kb2 generated on the basis of the second seed.

Please replace paragraph 3 at page 53, with the following rewritten paragraph:

As a result of the decryption process carried out at the step ~~S106~~ S108 by applying the block key Kb1, a decoded TS packet 304 is generated. A seed (seed 2) is then extracted from the decoded TS packet 304.

Please replace paragraph 4 at page 53 continuing onto page 54, with the following rewritten paragraph:

At a selector step S109 shown in Fig. ~~3~~ 11, the seed (seed 2) is extracted from the result of the decryption process by applying the block key Kb1. The extracted seed is supplied to a process carried out at a step S110 to generate a block key Kb2. Encrypted data obtained as a result of an encryption process applying the block key Kb2 are supplied to a decryption process carried out at a step S111 to generate a decrypted (unencrypted) result, which is then concatenated with the other result at a selector step 112.

Please replace paragraph 4 at page 55 continuing onto page 56, with the following rewritten paragraph:

Fig. 9 is a diagram showing a typical configuration in which both the seeds (seeds 1 and 2) are stored in the first TS packet 302 of the user data. In the typical configuration explained earlier by referring to Fig. 8, the seed (seed 1) 311 is included in the control data 301 while the other seed (seed 2) 312 is included in the first TS packet 302 at the head of the user data as encrypted information. In the typical configuration shown in Fig. 9, on the other hand, both the seed (seed 1) ~~321~~ 331 and the other seed (seed 2) 322 are stored in the first TS packet 302 at the head of the user data.

Please replace paragraph 3 at page 56 continuing onto page 57, with the following rewritten paragraph:

It is also possible to provide alternative welfare composition in which a flag included in the seed 321 stored at the head of the encryption processing unit is used for determining whether data has been encrypted in encryption processing units or has not been encrypted in encryption processing units. Figs. 10(a) and 10(b) are diagrams showing a further typical configuration in which the head of an encryption processing unit includes a seed. By using a flag recorded in a CCI portion serving as copy control information shown in Figs. 10(a) and 10(b), it is possible to determine whether or not data has been encrypted. If the data is determined to be encrypted data, the data is reproduced through a path of decryption of the data. If the data is determined to be unencrypted data, on the other hand, the data is reproduced without going through a path of decryption of the data.

Please replace paragraphs 2 and 3 at page 60, with the following rewritten paragraph:

As a result of the decryption process carried out at the step ~~S106~~ S108 by applying the block key Kb1, a decoded TS packet 304 is generated. A seed (seed 2) is then extracted from the decoded TS packet 304.

At a selector step S109 shown in Fig. 3, the seed (seed 2) is extracted from the result of the decryption process by applying the block key Kb1. The extracted seed is supplied to a process carried out at a step S110 to generate a block key Kb2. Encrypted data obtained as a result of an encryption process applying the block key Kb2 are supplied to a decryption process carried out at a step S111 to generate a decrypted (unencrypted) 305 result, which is then concatenated with the other result at a selector step 112.

Please replace paragraphs 1 and 2 at page 66, with the following rewritten paragraph:

As a result of the decryption process carried out at the step ~~S106~~ S108 by applying the block key Kb1, a decoded TS packet 304 is generated. A seed (seed 2) is then extracted from the decoded TS packet 304.

At a selector step S109 shown in Fig. 11, the seed (seed 2) is extracted from the result of the decryption process by applying the block key Kb1. The extracted seed is supplied to a process carried out at a step S110 to generate a block key Kb2. Encrypted data obtained as a result of an encryption process applying the block key Kb2 are supplied to a decryption process carried out at a step S111 to generate a decrypted (unencrypted) 305 result, which is then concatenated with the other result at a selector step 112.

Please replace paragraph 2 at page 72, with the following rewritten paragraph:

For example, Fig. ~~15~~ 16 is a diagram showing a configuration in which an information-processing apparatus 410 such as a PC is connected to an information-recording medium drive 420 for mounting an information-recording medium 430 such a DVD or a CD through an interface 411 on the information-processing apparatus 410 and an interface 421 on the information-recording medium drive 420. In this typical configuration, the information-recording medium drive 420 makes an access to the information-recording medium 430, transferring accessed data to the information-processing apparatus 410 such as a PC through the interfaces 421 and 411 and, in the information-processing apparatus 410, the data is reproduced.

Please replace paragraph 2 at page 77, with the following rewritten paragraph:

By adopting either of the methods described above, the two recording keys (REC keys) 1 and 2 are generated at the steps S554 and S555 respectively. Then, at a step ~~S556~~ S558, a process to generate a block key Kb1 is carried out.

Please replace paragraph 3 at page 81, with the following rewritten paragraph:

As a result of the decryption process carried out at the step ~~S556~~ S558 by applying the block key Kb1, a decoded TS packet 604 is generated. A seed (seed 2) is included in the decoded TS packet 604.

Please replace paragraph 1 at page 83, with the following rewritten paragraph:

The information-recording medium drive 510 and the information-processing apparatus 500 have the authentication keys Km 540 and 530 respectively. First of all, at a step S571, the information-processing apparatus 500 generates a random number Rb1 having a length of 64 bits and transmits the random number Rb1 to the information-recording medium drive 510. At a step S581, the information-recording medium drive 510 generates a random number Ra1. Then, at a step ~~S682~~ S582, an AES encryption process is carried out on the basis of joint data [Ra1 || Rb1] to generate a MAC (Message Authentication Code). The joint data [Ra1 || Rb1] is data obtained as a result of concatenation of the random number Ra1 and the random number Rb1. Let the MAC value be referred to as eKm (Ra1 || Rb1). It is to be noted that, in general, notation eKa (B) denotes a result of encryption of data B by using a key Ka, and notation A || B denotes a concatenation of data A and data B. The information-recording medium drive 510 transmits the generated MAC value eKm (Ra1 || Rb1) and the generated random number Ra1 to the information-processing apparatus 500.

Please replace paragraph 1 at page 85, with the following rewritten paragraph:

Furthermore, at a step S576, the information-processing apparatus 500 generates a random number Ra3 and transmits the random number ~~Ra3~~ Rb3 to the information-recording medium drive 510.

Please replace paragraph 3 at page 89 continuing onto page 90, with the following rewritten paragraph:

As described above, in this typical configuration where it is necessary to transfer a seed (seed 2) required for generating a key (a block key Kb2) to be applied to a process to decrypt an encrypted content as part of processing to reproduce data stored on an information-recording medium from a device to another, not only is the seed (seed 2) for generating the block key Kb2 encrypted before being transferred between the devices, but a recording key K2 is also encrypted before being transferred between the devices. Thus, even if data leaks from a transmission line between the devices, it will be difficult to acquire the seed (seed 2) and the recording key K2. As a result, difficulties to analyze a key generated by using the seed and analyze an encryption algorithm are increased so that protection of contents at a high level of security can be implemented. These features can be further strengthened through enhancement of confidentiality by implementing methods including the method of acquiring a recording key K1 to the method of computing a block key Kb1, the method of generating a session key Ks, and the method of encrypting the session key Ks in the information-recording medium drive ~~500~~ 510 as processing carried out in one LSI package.

Please replace paragraph 2 at page 95 continuing onto page 96, with the following rewritten paragraph:

A step S566 is a selector step to split a result generated at the step S565 into the decrypted seed (seed 2), data to be decrypted by using the block key Kb2, and unencrypted data. At a step ~~ZS567~~ S567 shown in Figs. 17 and 20, an AES encryption process based on the seed (seed 2) and the recording key K2 is carried out to generate a block key Kb2. The seed (seed 2) is a result of the decryption process carried out at the step S565 by applying the session key Ks. On the other hand, the recording key K2 is the key generated at the step S564.

Please replace paragraph 1 at page 97, with the following rewritten paragraph:

Also in this typical configuration, it is thus impossible to read out the seed (seed 2) from the disc or a data transmission line without decryption. As a result, difficulties to analyze a key generated by using the seed and analyze an encryption algorithm are increased so that protection of contents at a high level of security can be implemented. These features can be further strengthened through enhancement of confidentiality by implementing methods including the method of acquiring a recording key K1 to the method of computing a block key Kb1, the method of generating a session key Ks, and the method of encrypting the session key Ks in the information-recording medium drive ~~500~~ 510 as processing carried out in one LSI package.

Please replace paragraph 3 at page 103 continuing onto page 104, with the following rewritten paragraph:

Also in this typical configuration, it is thus impossible to read out the seed (seed 2) from the disc or a data transmission line without decryption. As a result, difficulties to analyze a key generated by using the seed and analyze an encryption algorithm are increased so that protection of contents at a high level of security can be implemented. These features can be further strengthened through enhancement of confidentiality by implementing methods including the method of acquiring a recording key K1 to the method of computing a block key Kb1, the method of generating a session key Ks, and the method of encrypting the session key Ks in the information-recording medium drive ~~500~~ 510 as processing carried out in one LSI package.

Please replace paragraph 4 at page 108 continuing onto page 109, with the following rewritten paragraph:

A processing unit includes the control data 711 having a length of 18 bytes and encrypted user data 701 having a size of 2048 bytes. A seed 674 is included in the control data 711. The encrypted data 701 is data encrypted by using a block key Kb1 generated on the basis of the seed ~~721~~ 674.

Please replace paragraph 2 at page 111, with the following rewritten paragraph:

Also in processing carried out in this typical configuration to reproduce data stored on an information-recording medium, data to be transferred from one device to another is encrypted by using a session key in advance. It is thus possible to prevent a content from leaking even if the encrypted data is tapped from a transmission line. As a result, protection of contents at a high level of security can be implemented. These features can be further strengthened through enhancement of confidentiality by implementing methods including the method of acquiring a recording key K1 to the method of computing a block key Kb1, the method of generating a session key Ks, and the method of encrypting the session key Ks in the information-processing apparatus ~~500~~ 650 as processing carried out in one LSI package.